Proposed Serial Switch Replacements

John Cory

Introduction:

The initial WTI Serial Port Switch selected for dial-in operations is no longer a viable solution due to heightened security requirements. More active security is necessary to meet ORDA system specifications. The replacement for the Serial Port Switch must have these capabilities:

- Unique ID's
- Authentication
- Auditing
- Out-of-bandwidth access through a dial-up modem
- Standard 19-inch rack mountable
- Occupy one rack unit
- Must support SNMP to facilitate proper communications with the APC Power Manager.

A couple of options are available to fulfill these requirements. The first of these is a basic model rack mount computer with both a modem and an extra PCI slot for a multi-port serial communications card. The simplest implementation of this option is on a 1U machine running the Linux operating system.

The other option is a commercially available console server. These devices allow RS-232 communications from a modem or LAN. Cynthia McDermott is still reviewing this solution for the security specification fulfillment.

A decision will be made after further investigation. A security TIM was held April 9th – minutes are attached.

Option #1: Rack-Mount Computer

Rack mount computers are commercially available through most major computer resellers, but only a few met the specifications needed. The biggest challenge is finding a 1U solution with two PCI card slots. Since rack mount solutions are geared toward high-powered servers, they have no on-board modem; therefore a PCI modem is required. For our application these servers are also more powerful than required for this project. However, the security on the units can be programmed into the OS to be very secure. Table I provides a list of a couple of options.

This is not our preferred option due to the fact that each module requires considerable setup time. Each unit would require a Linux OS load, installation of two pieces of hardware, and server/firewall configuration. The two pieces of hardware will include a 56k PCI modem and a multi-port serial card. The serial port card will be a Comtrol RocketPort 8 PCI, with 8 DB-9 connectors. This is the same card supplied with the RCP8.

Rack Mountable Computers	Speed (MHz)	# of PCI slots	Rack Units	Linux OS preloaded?	Authentication	Auditing	Unique ID	Price
Dell 1600	P3 1130	2	1	No	yes	yes	yes	$1950.00
IBM xSeries 305	P4 2000	2	1	No	yes	yes	yes	$1950.00

Table I: Rack Mount Computer Options & Feature Comparison

Option #2: Console Server

Console servers are embedded hardware devices that allow communication to RS-232 devices through a modem or network. They are available commercially through several resellers and manufacturers. RS-232 communications is through specially wired RJ-45 connectors. Therefore, special cabling would need to be procured to communicate properly with the required devices. Specifically, RJ-45 to DB-9 cables, wired according to the manufacturers specifications, would be required. Setup time would be less than that for the rack mount computer once the proper configuration is determined. Similar to Cisco routers already in the ORDA design, the servers require a config file to be downloaded to the Flash memory. As opposed to the rack mount computers in which the security can be guaranteed with the OS configuration, the security provided by the console server is still under investigation. Table II shows three different models that appear to meet the requirements.

The Unique ID and Authentication would occur in an Access Control List (ACL). This is a list of users and associated passwords verified for system access. The ACL is loaded into flash memory and preserved during power outages. Auditing is accomplished by storing events in a syslog file. A software syslog server process running on the RCP8 can alert all systems that a remote user has logged into the hardware console server, or has tried and failed.

There are several other useful security features integrated into certain console servers. Challenge Handshake Authentication Protocol (CHAP) is one of these features. CHAP allows a very secure control of logins. It challenges each attempted login for username and password. If this information is not entered correctly, the connection is terminated. Another security feature is Open SSH, or Secure Shell. This sets up a secure tunnel connection along which all information is encrypted. This prevents any outside sources to view login information.

	Lantronix SCS820	MRV LX-4008S-101AC	Cyclades TS800
OS	Redhat Linux	Linux	Monta Vista Linux
Internal Modem	Yes	Yes	Yes/PCMCIA
Size	1U	1U	1U
Unique ID	Yes	Yes	Yes
Password	Yes	Yes	Yes
Auditing	Yes	Yes	Yes
	Logs access to a syslog accessible by a syslog server on RCP8	Logs access to a syslog accessible by a syslog server on RCP8	Logs access to a syslog accessible by a syslog server on RCP8
PPP	Yes	Yes	Yes
CHAP	Yes	Yes	Yes
Access Control Lists	Yes	Yes	Yes
Open SSH v2	Yes	Yes	Yes
SNMP	Yes	Yes	Yes
Redundant power supply	Yes	No	Yes
Price	$2,031.50 without Bulk Discount	$1,600.00 without Bulk Discount	$1500.00 + modem with Bulk Discount
Number of Ports	8	8	8
Updates and Patches	Free updates and security fixes, released every 6-18 months based on urgency	Yearly cost of 8% of unit for updates, security patches free	Free quarterly updates and free security patches as they are released

Table II: Console Server Options & Feature Comparisons

Website Links:

Lantronix:
http://www.lantronix.com/products/cs/scs820_scs1620/index.html
MRV:
http://www.mrv.com/products/products.php?id=MRV-IR-008
Cyclades:
http://www.cyclades.com/products/?id=3&view=specifications

Conclusion

While the rack mount computers have a large number of customization options and can be very secure, they have a long setup time. The console

servers, on the other hand, have a short setup time and are engineered for this specific use. Since console servers are designed for out-of-bandwidth RS-232 communication, it provides us with an industry tested solution. The console servers also have a shorter depth than the rack mount computers. This means the console servers take up less space in the back of the rack, which allows easier wire routing in the cabinet. Table III shows a direct comparison of the pros and cons of both solutions.

	Pros	Cons
Rack mount Linux Computer	Broad Customization options Control though KVM	Long Setup Time Long Depth
Console Server	Quick and easy setup Designed for use in this area Shorter Depth	Specialty Cabling required Security still in question

Table III: Comparison between Rack Mount Computers & Console Servers

Given the information in Table III, the console server will provide a better solution than the rack mount computer. However, the security of the console server must be verified before a final decision can be reached. The shorter setup time required for the console server is a large driving factor in the decision, especially given the large number of systems that need to be installed. This helps to keep radar downtime to a minimum during deployment.